

Lab 4 - NAT Overload (PAT)

Lab 4: NAT lab — NAT overload

The physical topology is as shown in Figure 14–4.

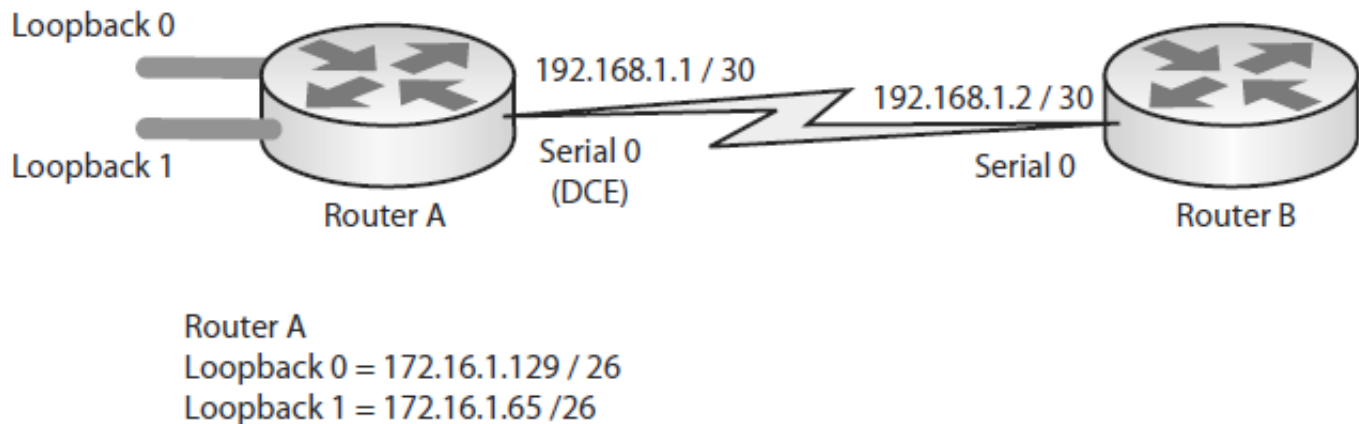


Figure 14–4: NAT overload

Lab exercise

Your task is to configure the network in Figure 14–4 to allow the hosts on the 172.16.1.128 subnet to access the Internet using the overloaded NAT address of 10.0.0.1. Hosts on the

172.16.1.64 subnet should not be natted. Please feel free to try the lab without following the lab walk-through section.

Purpose

Being able to configure NAT is a fundamental CCNA skill. Any client who needs to access the Internet will want to use NAT. The key is to understand the client's requirements and then design a solution to fit his needs. This lab helps you to understand NAT, access-lists, and VLSM.

Lab objectives

1. Use the IP addressing scheme depicted in Figure 14–4. Router A needs a clock rate on interface serial 0: set this to 64000.
2. Set telnet access for the router to use the local login permissions of username "banbury" and the password "ccna".
3. Put a static route on the router.
4. Configure the inside and outside NAT interfaces on the router.
5. Configure NAT overload.
6. Finally, test the NAT overload from loopback 0 and loopback 1.

Lab walk-through

1. To set the IP addresses for an interface, you will need to do the following:

```
Router#config t
Router(config)#hostname RouterA
RouterA(config)#
RouterA(config)#interface serial 0
RouterA(config-if)#ip address 192.168.1.1 255.255.255.252
RouterA(config-if)#clock rate 64000 « If this is the DCE side
RouterA(config-if)#no shutdown
RouterA(config-if)#ip nat outside « The outside NAT network
RouterA(config-if)#interface loopback 0 « No need for “no shutdown” on loopback interfaces
RouterA(config-if)#ip address 172.16.1.129 255.255.255.192
RouterA(config-if)#ip nat inside « The inside NAT network
RouterA(config-if)#interface loopback 1
RouterA(config-if)#ip address 172.16.1.65 255.255.255.192
RouterA(config-if)#ip nat inside
RouterA(config-if)# ^Z
RouterA#
```

Router B:

```
Router#config t
Router(config)#hostname RouterB
RouterB(config)#interface serial 0
RouterB(config-if)#ip address 192.168.1.2 255.255.255.252
RouterB(config-if)#no shutdown
RouterB(config-if)#exit
RouterB(config)#ip route 0.0.0.0 0.0.0.0 serial 0
RouterB(config)# ^Z
RouterB#
```

To set the clock rate on a serial interface (DCE connection only) you need to use the “clock rate #” command on the serial interface, where # indicates the speed:

```
RouterA(config-if)#clock rate 64000
```

Ping across the serial link now .

2. To set telnet access, you need to configure the VTY lines to allow telnet access: to do this type (from configuration mode):

```
RouterA(config)#line vty 0 4 « Enters the VTY line configuration
```

```
RouterA(config-line)#login local « This will use local usernames  
and passwords for telnet access
```

```
RouterA(config-line)#exit « Exit the VTY config mode
```

```
RouterA(config)#username banbury password ccna « Creates username  
and password for telnet access (login local)
```

Router B:

```
RouterB(config)#line vty 0 4
```

```
RouterB(config-line)#login local
```

```
RouterB(config-line)#exit
```

```
RouterB(config)#username banbury password ccna
```

3. To set the “enable password”, do the following:

```
RouterA(config)#enable secret cisco « Sets the “enable password” (encrypted)
```

Router B:

```
RouterB(config)#enable secret cisco
```

4. You need to configure a NAT pool and then tell the pool which access-list to access to determine what traffic you want to be NATted:

```
RouterA(config)#ip nat pool internet_out 10.0.0.1 10.0.0.1 prefixlength 24
```

The pool consists of one address

```
RouterA(config)#ip nat inside source list 1 pool internet_out overload
```

Tell the router to overload the pool (i.e. use PAT)

```
RouterA(config)#access-list 1 permit 172.16.1.128 0.0.0.63
```

Match any host on the 172.16.1.128 subnet

5. To see if NAT is working, we need to turn on a debug with “debug ip nat”. Now imagine that the loopback address of 172.16.1.129 is a host on the LAN that wants to get out to the Internet. When the packet from the NATted LAN passes through the router, it will match the access-list and be translated to the overloaded NAT address.

```
RouterA#debug ip nat
```

IP NAT debugging is on

RouterA#ping

Protocol [ip]:

Target IP address: 192.168.1.2

Repeat count[5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface: loopback0

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 40/41/40ms

RouterA#

00:43:59: NAT:s=172.16.1.129->10.0.0.1, d=192.168.1.2[20]

00:43:59: NAT:s=192.168.1.2, d=10.0.0.1->172.16.1.129[20]

00:43:59: NAT:s=172.16.1.129->10.0.0.1 d=192.168.1.2[21]

00:43:59: NAT:s=192.168.1.2, d=10.0.0.1->172.16.1.129[21]

00:43:59: NAT:s=172.16.1.129->10.0.0.1, d=192.168.1.2[22]

00:43:59: NAT:s=192.168.1.2, d=10.0.0.1->172.16.1.129[22]

00:43:59: NAT:s=172.16.1.129->10.0.0.1, d=192.168.1.2[23]

00:43:59: NAT:s=192.168.1.2, d=10.0.0.1->172.16.1.129[23]

00:43:59: NAT:s=172.16.1.129->10.0.0.1, d=192.168.1.2[24]

00:43:59: NAT:s=192.168.1.2, d=10.0.0.1->172.16.1.129[24]

RouterA#show ip nat tran « **Short for “translations”**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	10.0.0.1:8759	172.16.1.129:8759	192.168.1.2:8759	192.168.1.2:8759
icmp	10.0.0.1:8760	172.16.1.129:8760	192.168.1.2:8760	192.168.1.2:8760

icmp 10.0.0.1:8761	172.16.1.129:8761	192.168.1.2:8761	192.168.1.2:8761
icmp 10.0.0.1:8762	172.16.1.129:8762	192.168.1.2:8762	192.168.1.2:8762
icmp 10.0.0.1:8763	172.16.1.129:8763	192.168.1.2:8763	192.168.1.2:8763

RouterA#

00:44:59: NAT: expiring 10.0.0.1 (172.16.1.129) icmp 8759 (8759)

00:44:59: NAT: expiring 10.0.0.1 (172.16.1.129) icmp 8760 (8760)

00:44:59: NAT: expiring 10.0.0.1 (172.16.1.129) icmp 8761 (8761)

00:44:59: NAT: expiring 10.0.0.1 (172.16.1.129) icmp 8762 (8762)

00:44:59: NAT: expiring 10.0.0.1 (172.16.1.129) icmp 8763 (8763)

You can see from the NAT translation table below that the router is allocating ports for the translations, in this example, ports 8759 to 8763.

Now ping from loopback 1, which does not match the access-list because it is in a different subnet. The address should not be NATted.

RouterA#ping

Protocol [ip]:

Target IP address: 192.168.1.2

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface: loopback 1

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/37/60 ms

RouterA#show ip nat tran

RouterA#

6. Now please enter reload at the "Router#" prompt and type "yes" to confirm.

Show runs

RouterA#show run

Building configuration...

Current configuration : 757 bytes

!

version 12.1

no service single-slot-reload-enable

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

!

hostname RouterA

!

ip subnet-zero

!

interface Loopback0

ip address 172.16.1.129 255.255.255.192

ip nat inside

!

Interface Loopback1

ip add 172.16.1.65 255.255.255.192

ip nat inside

!

interface Ethernet0

no ip address

shutdown

!

interface Ethernet1

no ip address

shutdown

!

interface Serial0

```
ip address 192.168.1.1 255.255.255.252
ip nat outside
clock rate 64000
!
interface Serial1
no ip address
shutdown
!
ip nat pool internet_out 10.0.0.1 10.0.0.1 prefix-length 24
ip nat inside source list 1 pool internet_out overload
ip classless
no ip http server
!
access-list 1 permit 172.16.1.0 0.0.255.255
!
!
line con 0
line aux 0
line vty 0 4
!
end
```

RouterA#

- - -

RouterB#show run

Building configuration...

Current configuration : 456 bytes

!

version 12.2

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

```
!  
hostname RouterB  
!  
ip subnet-zero  
!  
interface Serial0  
ip address 192.168.1.2 255.255.255.252  
!  
interface Serial1  
no ip address  
shutdown  
!  
interface TokenRing0  
no ip address  
shutdown  
!  
ip classless  
!  
ip route 0.0.0.0 0.0.0.0 Serial0  
  
!  
no ip http server  
ip pim bidir-enable  
!  
line con 0  
line aux 0  
line vty 0 4  
!  
end  
  
RouterB#
```




© 2006-2011 HowtoNetwork.net All Rights Reserved. Reproduction without permission prohibited.